NATIONAL SCHOOL OF CYBERSECURITY

2024/2025

Lecturer: H. MOUFEK

# Algebra 1 - Tutorial 4

Basic Training Cycle

Algebraic Structures

## Exercise 1

Let $G = ]-1,1[$. We define for all elements $x$ and $y$ of $G$:

$$x * y = \frac{x+y}{1+xy}.$$

$\boxed{1}$ Verify that $*$ is an associative binary operation on $G$.

$\boxed{2}$ Show that $(G,*)$ is a group. Is it commutative?

$\boxed{3}$ Provide an expression for $x^{*n}$.

## ~~Exercise 2~~

We equip $\mathbb{R}^2 \setminus \{(0,0)\}$ with the binary operation:

$$(x,y) * (x',y') = (xx' - yy', xy' + x'y).$$

$\boxed{1}$ Show that $(\mathbb{R}^2 \setminus \{(0,0)\}, *)$ is a group on , and that the curve defined by the equation $x^2 + y^2 = 1$ is a subgroup of $\mathbb{R}^2 \setminus \{(0,0)\}$, which we will denote by $C$.

$\boxed{2}$ Show that $f : (x,y) \to x + iy$ is a group isomorphism from $\mathbb{R}^2 \setminus \{(0,0)\}$ into $\mathbb{C}^\times$, bijectively mapping $C$ onto the subgroup of complex numbers with modulus 1.

$\boxed{3}$ Show that $\theta \to (\cos(\theta), \sin(\theta))$ is a surjective group homomorphism from $\mathbb{R}$ to $C$. What is its kernel?

## Exercise 3

We denote by $\mathbb{Z}[\sqrt{3}]$ the set of real numbers of the form $a + b\sqrt{3}$, where $a, b \in \mathbb{Z}$.

$\boxed{1}$ Show that $\mathbb{Z}[\sqrt{3}]$ is a subring of $(\mathbb{R}, +, \times)$.

$\boxed{2}$ Show that the function

$$f : \begin{cases} \mathbb{Z}^2 & \to \mathbb{Z}[\sqrt{3}] \\ (a,b) & \mapsto a + b\sqrt{3} \end{cases}$$

is a group isomorphism from $(\mathbb{Z}^2, +)$ to the group $(\mathbb{Z}[\sqrt{3}], +)$.

$\boxed{3}$ For every $x \in \mathbb{Z}[\sqrt{3}]$, there exists a unique pair $(a,b) \in \mathbb{Z}^2$ such that $x = a + b\sqrt{3}$.

(a) For every real number $x = a + b\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ with $(a,b) \in \mathbb{Z}^2$, the conjugate of $x$, denoted $\tilde{x}$, is the real number $a - b\sqrt{3}$. Show that the function

$$g : \begin{cases} \mathbb{Z}[\sqrt{3}] & \to \mathbb{Z}[\sqrt{3}] \\ x & \mapsto \tilde{x} \end{cases}$$

is a ring automorphism.

(b) For every $x = a + b\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$ with $(a,b) \in \mathbb{Z}^2$, define $N(x) = x\tilde{x}$. Verify that for all $(x,y) \in (\mathbb{Z}[\sqrt{3}])^2$, $N(xy) = N(x)N(y)$.

(c) Show that $x \in \mathbb{Z}[\sqrt{3}]$ is invertible if and only if $N(x) = 1$ or $N(x) = -1$. What is its inverse in each case?